Первообразный корень

$\boxed{1}$ **Повторение.** Пусть $1 = d_1 < d_2 < \ldots < d_k = n$ — все делители числа n. Докажите, что $\varphi(d_1) + \ldots + \varphi(d_k) = n$.

Обозначим через $\psi(t)$ количество остатков от деления на p, чей показатель равен t.

$\boxed{2}$ Пусть p — простое число. $1 = d_1 < d_2 < \ldots < d_k = p - 1$ — все делители числа $p - 1$. Докажите, что $\psi(d_1) + \ldots + \psi(d_k) = p - 1$.

$\boxed{3}$ Пусть показатель остатка a по модулю p равен d.

(a) Докажите, что $1, a, \ldots, a^{d-1}$ — это все корни многочлена $x^d - 1$.

(b) Пусть показатель остатка b по модулю p также равен d. Докажите, что $b \equiv a^s \pmod p$.

(c) В условиях предыдущего пункта докажите, что НОД$(d, s) = 1$.

$\boxed{4}$ Выведите из предыдущей задачи, что $\psi(d) \leq \varphi(d)$ для любого делителя $d \mid (p - 1)$.

$\boxed{5}$ Докажите, что $\psi(d) = \varphi(d)$ для любого делителя $d \mid (p - 1)$.

Из задачи 5 следует, что $\psi(p - 1) = \varphi(p - 1) > 0$. Значит, существует остаток g (и не один, а целых $\varphi(p - 1)$ штук) такой, что показатель g равен $p - 1$. Такой остаток называется первообразным корнем по модулю p.

$\boxed{6}$ Для каких простых p первообразный корень может быть квадратичным вычетом?

$\boxed{7}$ Докажите, что любой ненулевой остаток a от деления на p представим в виде $a \equiv g^t \pmod p$ для некоторой степени t.

$\boxed{8}$ Сколько решений имеет уравнение

(a) $x^5 \equiv 1 \pmod{101}$?

(b) $x^{70} \equiv 1 \pmod{101}$?

(c) $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{101}$?

$\boxed{9}$ Найдите остаток $1^{10} + 2^{10} + \ldots + 100^{10}$ от деления на 101.

$\boxed{10}$ Пусть p — простое. Можно ли расставить по кругу числа $1, 2, \ldots, p - 1$ так, чтобы для любых трех подряд идущих чисел a, b, c (именно в таком порядке) число $b^2 - ac$ делилось бы на p?

$\boxed{11}$ Можно ли разбить числа от 1 до 2016 на группы по 7 так, чтобы сумма чисел в каждой семёрке делилась на 2017?